UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: INFORMATION ASSOCIATED WITH THE GOOGLE DRIVE ACCOUNT USERNAME MIKE.CLEMENCE@GMAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC, 1600 AMPHITHEATRE PARKWAY, MOUNTAIN VIEW, CA 94043.	Case No. 21-mj- 148-01-AJ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ronald Morin, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (HSI), being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Google Drive Account username mike.clemence@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a technology company that specializes in internet related services, with offices at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Department of Homeland Security,

Immigration and Customs Enforcement, Homeland Security Investigations (HSI), and have been so employed since May 2006. I am currently assigned to the Manchester, New Hampshire field office. As part of my regular duties as an agent, I investigate criminal violations relating to a broad range of immigration and customs related statutes, including those relating to child exploitation and child pornography. I have received training in the area of child pornography and child exploitation, and as part of my duties have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. §2256) in various forms of media, including digital/computer media. I have conducted investigations and executed search warrants involving child exploitation and child pornography offenses.

3. I am a "Federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The statements in this affidavit are based on my own investigation of this matter as well as on information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. While I have included all material facts relevant to the requested search warrant, I have not set forth all of my knowledge about this matter.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. § 2252(a)(4)(B) have been committed and that there is probable cause to believe that fruits, evidence, and instrumentalities of the Specified Federal Offenses are likely to be found in the Google Drive Account, as set forth below.

SPECIFIED FEDERAL OFFENSES

6. Title 18, United States Code, Section 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:

a) "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and

other mobile devices. See 18 U.S.C. § 1030(e)(1).

c) "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

d) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f) A "storage medium" is any physical object upon which computer data can be

recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

g) "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

h) The "Darknet" is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization, and often uses a unique customized communication protocol.

i) The "Tor network" or "Tor" is free and open-source software for enabling anonymous communication by directing Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Tor is available to Internet users and is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

j) A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor anonymity network.

k) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l) An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

m) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

PROBABLE CAUSE

8. In February 2020, the HSI Manchester, NH, office received information that originated from a foreign law enforcement agency known to the Federal Bureau of Investigation (FBI) and with a history of providing reliable, accurate information in the past. In part, the information provided by the foreign law enforcement agency specified that on April 28, 2019, at 20:25:08 UTC, an individual originating from IP address 65.175.213.176 accessed a known

Darknet web site that facilitated the sharing of child sex abuse and exploitation material with a particular emphasis on sexually explicit material depicting young boys. Users of the website were able to view some material without creating an account. However, an account was required to post and access all content.

9. According to publicly available information, IP address 65.175.213.176 is owned and operated by Atlantic Broadband. On or about September 9, 2019, a summons was served on Atlantic Broadband for subscriber information associated with the IP address on April 28, 2019 at 20:25:08 UTC. Atlantic Broadband provided the following subscriber details:

a. Subscriber name: Michael Clemence

b. Service and billing address: 27A Crow Hill Road, Rochester NH

c. Phone numbers: 480-694-7209, 603-507-0703

10. A query of publicly available databases for information related to Michael Clemence revealed the following: year of birth 1985; last known address: 31 Adams Avenue, Rochester, NH. The queries also indicated that Michael Clemence is married to Elizabeth Clemence and has two young children.

11. CLEAR records identified Michael Clements' date of birth as [REDACTED]/1985, SSN [REDACTED], address 31 Adams Ave. Rochester NH, email address enderwigman@msn.com. Criminal history checks revealed no derogatory information. Property record checks indicated that he purchased the Adams Ave. property on 10/28/2019 with Elizabeth Anne Clemence.

12. On May 26, 2021, SA Mike Perella, Sean Serra, and Derek Dunn conducted a consensual knock and talk with Michael Clemence ("Clemence") at 31 Adams Ave in Rochester. Clemence answered the door and agents identified themselves. SA Perella advised Clemence

that agents were at his residence to ask about certain internet activity that occurred in April of 2019 at his previous residence, 27A Crow Hill Rd. in Rochester. Clemence expressed suspicion at the reason for agents' presence and advised that he had consumed a couple of beers. Clemence advised that his wife, Elizabeth, was at work.

13. During the conversation, Clemence volunteered that the tenant that lived next door to him at 27A Crow Hill Drive was an IT specialist and had done some IT work for him. Clemence identified this neighbor as "Kevin," and advised that "Kevin" had since moved to Maine. Clemence was vague about the nature of the IT work "Kevin" had done for him in the past.

14. Agents advised Clemence that they were investigating internet activity associated with child exploitation material, and that some of this activity occurred in April 2019 from the IP address associated with his previous residence on Crow Hill Rd. Clemence expressed vague familiarity with the dark web, offering that he understood that it was used to buy and sell illegal drugs. When asked, Clemence denied any knowledge of Tor.

15. Clemence then described an event that took place around that same time in 2019 in which his wife was looking on their laptop and she viewed something that appeared to be "really bad." Clemence relayed that his wife was very alarmed at what she saw on the computer and she did not know what it was or how it got onto the computer. Clemence did not elaborate or provide specifics about what his wife had observed on the computer. After observing this material on the computer, he and his wife "wiped" the computer and gave it to a family friend.

16. Agents asked Clemence about the computer he currently had. In response, Clements stated that he had a computer that he used for work and offered to allow agents to conduct a manual review of this computer. A manual review was conducted onsite, and no illicit

material was observed. Agents left their contact information with Clemence and advised that they would like Clemence's wife to contact them to arrange an interview. Clemence's wife, Elizabeth Clemence ("Elizabeth") contacted agents the following day and eventually made arrangements to be interviewed at her home on June 4, 2021.

17. On June 4, 2021 SA Mike Perella and I returned to the SUBJECT PREMISES at approximately 10:44 a.m. to conduct a consensual interview of Elizabeth Clemence. Elizabeth disclosed that on May 18, 2019, she was printing church documents from a household computer and accessed a folder titled "Documents." She advised that the computer was a Dell laptop that belonged to her husband, but that they both used the computer. Within the "Documents" folder, she saw approximately 14,000 images and videos of what appeared to Elizabeth to depict child pornography. She described one file as two naked boys in a bathtub. In addition, Elizabeth advised that the filenames that she observed were consistent with child pornographic material. This occurred when they were living on Crow Hill Road in Rochester. Elizabeth advised that their internet connection at that home was secure and that nobody had the password.

18. When Elizabeth confronted Clemence about what she found on the computer, he stated he didn't know how it got there and suggested that their computer must have been hacked. Elizabeth explained that she and Clemence did not know what to do about the material she had located on their computer. They considered going to the police, but at the time they were exploring the possibility of fostering children and they were concerned about jeopardizing their ability to do so. As a result, they decided to wipe the hard drive themselves. They also changed the passwords to the computer and the wireless internet. Elizabeth recalled it was possible that their neighbor, Kevin Mayfield, helped them change the password for the internet. They subsequently called an attorney the following Monday, and the attorney purportedly concurred

that it was good they wiped the hard drive. Elizabeth advised that she and Clemence were very concerned about the incident when it occurred and that they talked about it with their pastor and several close friends.

19. Elizabeth advised that at the beginning of the pandemic, a couple that they were friends with from church, Drew and Sarah Lytle, were in need of a computer for Zoom meetings. Elizabeth and Clemence decided to give them their Dell laptop computer. Prior to giving the computer to the Lytles, Elizabeth and Clemence wiped the hard drive a second time. The Lytles gave the computer to their eldest son. Elizabeth advised that the Lytles live in Lebanon, Maine, and advised that after speaking with agents the week of May 26, 2021, Clemence did retrieve the Dell laptop computer from the Lytles.

20. Elizabeth advised that when she learned from Clemence that agents had been at their residence the previous week and learned the nature of their investigation, she checked all of the thumb drives in the house for the presence of child pornography. She did this without Clemence's knowledge. She advised that she did not locate anything that appeared to be child pornography. Elizabeth further disclosed that she and Clemence have an "open marriage" in the sense that they share access to each other's online accounts, including email, social media, financial accounts, etc. They also share access to the electronic devices in the home.

21. Agents asked Elizabeth whose name the internet service was in at their previous address on Crow Hill Road. Elizabeth left the room to consult her records and returned with some paper files. Agents also inquired about who paid the bills, took care of household finances, etc., and Elizabeth stated that she did. Agents inquired whether she recalled any unusual or suspicious purchases around the time of April or May 2019 when this activity occurred. She indicated she could not recall anything offhand, but asked if she could consult her records. She

left the room and returned with a laptop computer, which she used to access her financial accounts and did not find anything noteworthy.

22. Elizabeth asked whether there was anything else that she should "look for," and agents explained that they could not direct her to do any specific searching of Clemence's devices or accounts. However, they advised that there were certain applications and cloud storage accounts that are commonly encountered in these types of investigations. Elizabeth stated that Clemence did have a cloud storage account that she also had access to and stated that she was "on it right now." Agents advised Elizabeth that if she encountered anything concerning in the accounts to which she and her husband shared access, she could contact them. Agents left their contact information and departed the residence.

23. A short time later, while agents were en route back to their office, I received a telephone call from Elizabeth Clemence. Elizabeth disclosed that while reviewing the contents of Clemence's Google cloud account, she observed approximately four videos that appeared to depict child pornography. She described one such video as two male children that were clothed and spanking each other. Another video appeared to depict two young boys, approximately 13 years old, performing oral sex on each other. She later described a third video in which it appeared that an adult male was engaged in anal penetration of a prepubescent boy that appeared to be approximately 10 years old. The boy was blindfolded and had something over his mouth.

24. Elizabeth advised that the cloud storage account is connected to her husband's Gmail account, which is mike.clemence@gmail.com and that both the email address and password, both of which she has access to, are required to login to the Google cloud account. Elizabeth further stated that Clemence had access to his Gmail account on his cell phone.

25. Upon learning this information, agents determined that they would return to the

residence and secure it so that they could seek a search warrant. Agents arrived back at the residence at approximately 2:50 pm and observed a red Honda Civic with NH registration 3936669 parked in the driveway. Clemence was seated in the driver's seat with the driver's door ajar and one foot out the door. Clemence appeared to have his cell phone in his hand. When agents parked their vehicle, Clemence exited his car, leaving the door ajar, and placed his cell phone on the front passenger seat. SA Perella observed the cell phone in plain view on the vehicle seat and noticed that the screen was illuminated and it appeared that a video was playing. SA Perella asked Clemence whether the cell phone on the seat was his, and Clemence confirmed that it was. SA Perella advised Clemence that agents would be securing the phone so that they could apply for a search warrant for its contents.

26. Clemence was extremely agitated and upset that agents had seized his phone. Agents explained that additional information had come to light since their interview with him the previous week. Agents explained that Clemence was not under arrest and that he was free to leave. Agents advised Clemence of his rights, and Clemence advised that he would like to speak with a lawyer. Agents offered the use of their own cell phones in order to allow Clemence to contact his attorney, but Clemence refused and insisted that he needed his own cell phone in order to get his attorney's contact information. Eventually, Clemence's wife provided a business card with their attorney's phone number on it, but Clemence still declined to use agents' phones to call his attorney. He left the residence in his vehicle a short time later.

27. I reviewed two of the videos that Elizabeth previously described to me over the phone that appeared to Elizabeth to depict child pornography. Based on my training and experience, I agree that they appeared to depict child pornographic material. Elizabeth also described a concerning photograph of her 3 year old son that she found in Clemence's Google

Drive account. She stated that her son was depicted naked from the waist down facing the wall. It appeared to have been taken in the basement of the home and depicted her son's buttocks. Elizabeth explained that Clemence is responsible for disciplining the children, and stated that when he does so he takes them to a private area of the house.

28. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 2252(a)(4)(B), relating to possession and access with intent to view child pornography, will be located in the Google Drive account referenced herein and more particularly described in Attachment A.

29. On June 4, 2021, a preservation letter was served on Google Inc. for the Google Drive associated with the username mike.clemence@gmail.com. The preservation letter alerts Google that additional legal service may be sent requesting information about this account. Once Google receives the preservation letter, they preserve a "snapshot" of the account from the day the letter is received.

30. Based on my training and experience I know that Google Drive is a file storage and synchronization service operated by Google. It allows users to store files in the cloud, synchronize files across devices and share files. It is available on the internet and as a mobile application. Google Photos is a photo sharing and storage service developed by Google. It is available both on the internet and as a mobile application. It gives users free unlimited storage space for photos and videos. Google Photos can be configured to automatically sync photos and videos taken with a user's camera to a user's Google Drive account.

31. In my training and experience, I know that Google is an online content website that was launched on the internet in 1998. Since their debut Google currently maintains a variety of online content products and services and they are ranked as one of the most frequently visited

web sites in the United States. Additionally, Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

32. I know that Google allows users to create a free Google account that will provide various types of services. When a Google user accesses the different types of services and activities data is created. By default, Google stores that data for each account user. A user may access their Google account and delete information or turn off various services, but that requires a proactive step by the user. Google accounts have an area that Google refers to as My Dashboard. My Dashboard is accessible by a user by going to https://myaccount.google.com/mydashboard, once the user is logged into his or her individual Google account. My Dashboard contains an index of data stored by the user accessing the products made available by Google. This information includes: the name of the Google account holder, the google email address of the account holder, searches run using the Google search engine by the account holder, a record of the types of devices used to access the Google account, "Allo" Google assistance, Cloud Print, Google Books, Google Audio, Google Drive, Google

conversations, Google Chrome, Google Chrome Sync, Google Photos, Google Groups, Calendar, Contacts, Keep, Location History, Maps (your places), My Maps, Google Voice, Google Wallet, Play Store, Profile, and Youtube.

33. In addition to the above products, with the advent of smart phones and tablet devices, Google has developed an operating system that works on any android device. Any user who wishes to add software applications to that device must use the Google online store to complete the purchase or free download. Google stores the make, model, and International Mobile Equipment Identifier number (IMEI) or Mobile Equipment Identifier (MEID) of any device attached to any Google products.

34. The following are some of the products offered by Google, and the location of potential data to be recovered:

Google Account:

35. Google maintains information about their customers including primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers.

Google Drive:

36. Google provides a variety of on-line services, including electronic mail ("e-mail") access referred to as Gmail, and online storage such as Google Drive, or Google Photos available to the general public. Subscribers obtain an account by registering with Google. Google Drive is a file storage and synchronization service operated by Google. It allows users to store files in the cloud, synchronize files across devices and share files. It is available on the internet and as a mobile application. Files and folders stored in Google Drive can be shared privately with particular users having a Google account, using their @gmail.com email address.

37. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and on other Google files/services such as Google Drive, or Google Photos. Google provides 15 GB of free Google online or cloud storage to any Google user.

38. Subscribers to Google might not store on their home computers copies of the e-mails, images, documents, or videos stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

Google Docs:

39. Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. I believe this information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales,

communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation.

Google Photos:

40. Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device. In many cases, a cellular telephone user may configure their device to automatically upload pictures taken with a mobile device to their Google Drive account. Google uses image recognition software on the photos and will organize them by date, time, location or subject matter. On the main image page Google groups the photos by the subject matter. Google software creates models of the face in the user's photos in order to group similar faces together. A Google user may create photo library and label it, for example "mom" which would contain any images of the user's mother. The label is private to the user and is not seen by anyone with whom the user shares the photos. Photos and Videos of the user are backed up to the user's Google Drive account. However, the user can change or select a different account to back up the photos. Users may also delete any photos that have been previously taken from the device, and store them only in the Google Cloud. Google will also allow users to store images and videos from third-party applications, for example Instagram, Facebook or messaging apps. Additionally, Google photo will hold onto any photos that have been deleted for a period of 60 days. Google Takeout allows users to download all of his or her photos from the Google Cloud.

Google Hangouts:

41. Google created a unified communications service that allows members to initiate and participate in text, voice, or video chats, either one-on-one or in a group. Hangouts are built

into Google+ and Gmail, and mobile versions are available for iOS and Android devices. Users of Google Voice have the ability to use Hangouts to make free domestic calls from any computing device.

Google Calendar:

42. Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. I believe this information will identify relevant dates and appointments germane to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses.

Google Contacts:

43. When a user links their Android device to their Google account the names, addresses, phone numbers, email addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process is continuously updates so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. I believe this information is pertinent to the investigation as it will assist with identifying previously unknown co-conspirators, victims, and/or witnesses.

Google Search History:

44. Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user selected results. Furthermore, these searches are differentiated by the specific type of search a user performed into categories. These categories include a general web search, and specialty searches where the results are focused in a particular group such as images,

news, videos, and shopping. I believe a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it.

Google Chrome:

45. Google Chrome is the web browser that was created by Google. Google Chrome allows users to bookmark websites, control search history to all devices for a Google user. Google Chrome has settings that allow the Google user to control the privacy settings of the Google Chrome web browser. Google allows the individual Google user to customize the appearance of Google Chrome. I believe that a review of the history, bookmarks, web searches, privacy settings of the Google Chrome web browser will reveal information and evidence relevant to the ongoing criminal investigation.

Google Keep:

46. Google has created a product that allows users to create, organize and save notes, lists or ideas. These notes and lists may be shared with other users. Google Keep works on any device that has Internet access and allows for connection to the Google network.

Google Chrome Sync:

47. Google allows Google users of the Chrome Web browser to sync data across different devices. This service allows for the bookmarks, history, passwords and other settings to be the same on each device. I believe that this information will help demonstrate the identity of the account holder as well as the user tendencies and settings to assist in providing relevant information to the ongoing criminal investigation.

Google Location History:

48. Google collects and retains location data from any Google enabled mobile device. This includes Android and iPhone devices. The company uses this information for location based advertising and location based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access. I believe this data will show the movements of the suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation.

Google My Maps:

49. Google provides a service where a Google user can create a custom map to share and publish online. A user can create a map, add lines, shapes or placemarks, import geographically specific data including addresses, place names, or latitude and longitude coordinates. A Google user can add layers to the map to hide or highlight specific types of content. I believe this data will show potential maps created by the suspect to place the suspect at a location relevant to the ongoing criminal investigation.

Google+:

50. In 2011 Google introduced the social media web site Google+. Google+ offers many of the same popular features as other social media web sites and currently has over 170 million user profiles. Google+ shares many of the same account management features of Google including account management, access logs, data retained and information collected.

51. I know that Google+ allows an individual to create an account with his or her own page called a profile. Google+ profiles can include a short biography, photos of themselves and location information. Google+ also allows their users to send and receive messages, upload and link video and interact with other users through video conferencing. These features are described in more detail below:

52. A Google+ user can interact with other Google+ users in many ways. To send messages to users, post information, comment on hosted videos or upload videos to the site an individual must register for an account within the web site. To create a user account for Google+ an individual is transferred to Google.com and must create a user account within the Google network. Once an individual creates an account with Google the individual may also change this username, password, and name without having to open a new Google account.

53. Google asks individuals to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user account, Google may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Google account.

54. An individual with a Google+ account can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or

cover photo for his or her account page. In addition, Google+ users can post "bios" and other information to their profile pages.

55. Google also keeps IP logs for each user of the Google+ web site. These logs contain information about the user's logins to Google+ including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

56. Google+ users can post text, images, videos and links to external web sites within their profile for others to view in an area called their "Stream".

57. Google+ users can use their user accounts to post messages to their profiles for others to view. Individuals can also use their Google+ accounts to send messages to their "Circles". A Google+ "Circle" is a distribution list that a user maintains and organizes. A user can add, remove or censor a member of a particular "Circle" or several "Circles". Within a "Circle" a user can send and receive messages with other users, post photographs, videos and links to external web sites.

58. Google+ users can initiate a "Hangout" which is an area to initiate video conferencing with several other Google+ users. Within a "Hangout" a Google+ user is able to interact with other users in a live real-time format or they are able to create a webcast that is hosted by Google+. Webcasts created in Google+ can be stored in a Google+ user's profile and can be retrieved, shared and rebroadcasted at anytime. Whenever a Google+ user initiates a "Hangout" session, Google+ generates a unique URL that can be shared with others so that they can view the session. Or the "Hangout" can be broadcasted and stored on YouTube.

59. A Google+ user is also able to search using the Google.com search engine within the web site in a feature called "Sparks". "Sparks" is a front-end to Google Search, enabling users to identify topics they might be interested in sharing with others. "Featured interests"

sparks are also available, based on topics others globally are finding interesting. Sparks helps to keep users informed of the latest updates on the topics of their interest.

60. An individual can also access the Google+ web site through mobile applications that allow an individual to use the aforementioned features of Google+ through a mobile device such as a smart phone, and cellular telephone. An individual using a mobile device can communicate with other users through an application called "Messenger". "Messenger" facilitates communication and the sharing of media between users through a smart phone application or through standard short messaging service (SMS) messaging.

61. A Google+ user can also use their mobile device to broadcast location data to the Google+ web site to use Google+ Local. Google+ Local users broadcast location data submitted to the web site to reveal trending information, restaurants, popular businesses and items of interest based on information stored on a user's particular profile.

62. Google+ offers a wide variety of privacy settings that allow a user to expand or restrict the amount of information that is visible on their profile to friends or the general public. Regardless of the privacy settings selected by the User, the User's information is shared with Google.com and Google.com's marketing affiliates.

63. If a Google+ user does not want to interact with another user on Google+, the first user can "block" the second user from following his or her account.

64. Google+ users can connect their Google+ accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Google+ profiles.

65. Google users have the ability to store location data information about where users have been, trips users have taken, searches users have run in the Google Maps application under

Google Maps/Timeline. This data is being stored unless the user actively disables location history on the device and in the timeline application. If the service is enabled, it is actively connecting to GPS satellites in order to provide instant location data for a user. This data may be recoverable for a period of years through the user profile information stored with Google.

66. In some cases, Google+ users may communicate directly with Google and Google+ about issues relating to their account, such as technical problems or complaints. Social-networking providers like Google+ typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Google+ may also suspend a particular user for breaching Google's terms of service, during which time the Google+ user will be prevented from using Google+ services.

67. Therefore, the computers of Google are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Google+, such as account access information, transaction information, and other account information.

68. I know that individuals involved in the commission of criminal acts often utilize technology such as cellular telephones, smart phones, personal data assistants, laptop computers, personal media players, handheld radios, radio broadcast scanners and social media websites such as Google+ in order to: plan and discuss criminal activities, coordinate the movement of persons involved or property utilized or taken from a location and to relay information about law enforcement officials during the commission of a criminal act.

69. People who commit criminal offenses together often communicate prior to or following that crime. It is common for people to communicate via Google+ postings, emails and

private messages. Individuals who have committed crimes or who are closely associated with such people often communicate about the details of what occurred (the crime itself), the stress/angst relating to the event, the quality and quantity of evidence possessed by the authorities, and fears about being apprehended.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

70. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google LLC to disclose to the government copies of the records and other information particularly described in Attachment B. Upon receipt of the information described in Attachment B.I., government-authorized persons will review that information to locate the items described in Attachment B.II.

CONCLUSION

71. Based on the foregoing, I submit that probable cause exists that evidence of violations of 18 U.S.C. Section 2252(a)(4)(B) will be found in the Google Drive account associated with username mike.clemence@gmail.com.

72. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

73. THEREFORE, based on the foregoing, I request that this Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

/s/ Ronald Morin
Special Agent Ronald Morin
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Jun 7, 2021**

Time: 5:06 PM, Jun 7, 2021

Andrea K. Johnstone
U.S. Magistrate Judge
District of New Hampshire

ATTACHMENT A
ITEMS TO BE SEARCHED

This warrant applies to information associated with Google Drive Account username mike.clemence@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a technology company that specializes in internet related services, with offices at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Google LLC or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google LLC is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. Any and all photographs, videos, visual depictions or other content stored in Google Drive account username mike.clemence@gmail.com and all information pertaining to the source of such photographs, videos, visual depictions, messages, and other stored content from the inception of Google Drive account mike.clemence@gmail.com to the current date, including any and all photographs, videos, visual depictions, or other content that the user may have deleted or attempted to delete but that are still maintained and/or preserved by Google LLC.;

2. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone numbers and other personal identifiers;

3. All past and current usernames, account passwords, and names associated with the account;

4. Any communications, photos, videos or documents tending to establish the identity of the individual who uses and controls the Google account;

5. Any telephone numbers which have been registered with Google for the purposes of sending and receiving messages and for accessing Google+ through mobile applications;

6. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

7. All IP logs and other documents showing the IP address, date, and time of each login to the account;

8. All IP logs and other documents showing the IP address and/or telephone number, date, and time of each message send to and from to the account;

9. All device information for any make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device or target account.

10. All data and information associated with the profile page, including photographs, videos, "bios," and profile backgrounds and themes;

11. All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitee;

12. Contacts: All contacts stored by Google including name, addresses, notes, all contact phone numbers, email addresses, social networking links and images;

13. Docs (Documents): All Google documents including by way of example and not limitation, Docs (a web-based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web-based presentation program.) Documents will include all files whether created, shared, or downloaded;

14. Google Photos: All images, graphic files, video files, and other media files stored in the Google Photos service in their original file format for the account;

15. Location History-All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period July 1, 2013, to June 4, 2021;

16. All data and information that has been deleted by the user that is stored on any Google server or network;

17. A list of all of the people that the user maintains in Circles and all people who maintain the user in their Circles;

a. A list of all users that the account has blocked;

b. All privacy and account settings;

18. All records of Google searches performed by the account, including all past searches saved by the account from the period July 1, 2013, to June 4, 2021;

19. Any and all location data and information from the use of GoogleMaps, including but not limited to routes taken, check in data, points of interest selected, map searches, and any information related to places, timeline, traffic, and settings.

II. Information to be seized by the government

All information described above in Section I that constitute fruits, evidence and instrumentalities of violations of Title 18 U.S.C. § 2251(a) and 18 U.S.C. § 2252(a) involving Google Drive account username mike.clemence@gmail.com, during the time frame of the inception of this account up to the current date, for the account or identifier listed on Attachment A, including information pertaining to the following matters:

a. Any and all photographs, videos, visual depictions or other content related to the sexual exploitation of minors, including but not limited to communications and other content evidencing the actual and attempted sexual exploitation of minors, the distribution, receipt, and possession of child pornography, and the identification of any individuals involved in the same. This would include non-contraband images of minors and other individuals depicted in these images that may assist in the identification of minors who may be the victim of child exploitation or the suspects who are exploiting them.

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.